数理解析研究所講究録
411巻 1981年 27-61

Leopoldtの予想について

名大 教養部　三宅 克哉

代数体の単数に関するLeopoldtの予想は，虚2次体のアーベル拡大体の部分体についてすべての素数pに対して正しいことがBrumer[2]によって証明された。彼はAx[1]の分析に基づいて，代数的数に対するp-進対数関数の値の超越性をBakerにならって検証することに成功したのであった。

この小論では，まずIでLeopoldtの予想を紹介し，IIで岩沢の$\mathbb{Z}_p$-拡大との関係を見，IIIではAxの分析を拡大展開して，代数体の自己同型の群の作用に基づく分析とBrumerの結果とを組合せる。最後のIVにおいては虚2次体kのガロワ拡大Fについて，その単数群から得られる$Gal(F/k)$-加群の構造を分析し，Fがkのアーベル拡大であるときにはどのようにBrumerの超越的結果が適用できるかを見るとともに，ある種の非アーベル的な拡大F/kに対してもそれが適用されることを示す。

I. Leopoldt の予想

1. 有限次代数的数体 F の整数全体のなす環を $\mathcal{O}_F$ とするとき，これの正則元全体 $\mathcal{O}_F^\times$ が F の単数群である。この構造は，F に含まれる 1 の巾乗根全体のなす有限巡回群 W_F と，自由 $\mathbb{Z}$-加群 E とによって $\mathcal{O}_F^\times = W_F \times E$ と表わされており，E の $\mathbb{Z}$ 上の階数 r は $r = r_1 + r_2 - 1$ として得られている。ここに r_1, r_2 は

$$(*) \qquad F \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$$

によって定まる。（Dirichlet の単数定理。）

さて $\lambda_0 : (\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2})^\times \longrightarrow \mathbb{R}^{r_1+r_2}$ を

$$\lambda_0(x_1, \cdots, x_{r_1}, y_1, \cdots, y_{r_2}) = (\log|x_1|, \cdots, \log|x_{r_1}|, 2\log|y_1|, \cdots, 2\log|y_{r_2}|)$$

によって定め，さらに $\lambda : F^\times \longrightarrow \mathbb{R}^{r_1+r_2}$ を

$$F^\times \hookrightarrow (F \otimes_{\mathbb{Q}} \mathbb{R})^\times \cong (\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2})^\times \xrightarrow{\lambda_0} \mathbb{R}^{r_1+r_2}$$

によって定義すれば，$\mathbb{R}^{r_1+r_2}$ の部分空間

$$\{(z_1, \cdots, z_{r_1+r_2}) \mid z_1 + \cdots + z_{r_1+r_2} = 0\}$$

は丁度 $\lambda(N_{F/\mathbb{Q}}^{-1}(1))$ の $\mathbb{R}^{r_1+r_2}$ での閉包になっている。ただし $N_{F/\mathbb{Q}} : F^\times \longrightarrow \mathbb{Q}^\times$ は $F/\mathbb{Q}$ のノルム写像である。しかも $\lambda(\mathcal{O}_F^\times) = \lambda(E)$ がこの部分空間の格子になっている。

特に E の $\mathbb{Z}$ 上の生成元 $\varepsilon_1, \cdots, \varepsilon_r$ をとるとき，r_1+r_2 次の正方行列

$$\begin{pmatrix} \lambda(\varepsilon_1) \\ \vdots \\ \lambda(\varepsilon_r) \\ 0\ 0 \cdots 0\ 1 \end{pmatrix}$$

の行列式は0でなく；その絶対値R_Fは（Eと）$\varepsilon_1, \cdots, \varepsilon_r$のとり方によらず定まり，Fの単数基準と呼ばれる。

2. 上の(*)の左辺の$\mathbb{R}$は$\mathbb{Q}$のアルキメデス的附値による完備化であるが；これを$\mathbb{Q}$のp-進附値による完備化$\mathbb{Q}_p$でおきかえよう。Fの素イデアル$\mathfrak{p}$に対してFの$\mathfrak{p}$-進完備化を$F_{\mathfrak{p}}$とすれば

$$F \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \bigoplus_{\mathfrak{p}|p} F_{\mathfrak{p}}$$

となる。さて$\mathcal{O}_{\mathfrak{p}}$を$\mathcal{O}_F$の$F_{\mathfrak{p}}$における閉包とすれば，$W_{\mathfrak{p}}$を$F_{\mathfrak{p}}$に含まれる1の$(N_{F/\mathbb{Q}}(\mathfrak{p})-1)$乗根全体とするとき

$$\mathcal{O}_{\mathfrak{p}}^{\times} = W_{\mathfrak{p}} \times (1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}}).$$

しかも$\mathfrak{p}$-進対数関数 $\log : (1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}}) \longrightarrow F_{\mathfrak{p}}$ が級数

$$\log x = -\sum_{n=1}^{\infty} \frac{1}{n}(1-x)^n$$

によって定義される。また $\log(x \cdot y) = \log x + \log y$ が成り立ち，したがって $\log(W_{\mathfrak{p}}) = 1$ と見るのが自然であるから，これにより $\log$ が $\mathcal{O}_{\mathfrak{p}}^{\times}$ 上の関数と見なせる。

さてΩ_pを$\mathbb{Q}_p$の代数的閉包の完備化とすれば，自然なうめ込み

$$\lambda_0 : F \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_p \cong \bigoplus_{\mathfrak{p}|p} F_{\mathfrak{p}} \longrightarrow F \underset{\mathbb{Q}}{\otimes} \Omega_p \cong \Omega_p^{[F:\mathbb{Q}]}$$

がある。そこで $\lambda : \mathcal{O}_F^\times \longrightarrow \Omega_p^{[F:\mathbb{Q}]}$ を

$$\mathcal{O}_F^\times \hookrightarrow \prod_{\mathfrak{p}|p} \mathcal{O}_{\mathfrak{p}}^\times \xrightarrow{\log} \bigoplus_{\mathfrak{p}|p} F_{\mathfrak{p}} \xrightarrow{\lambda_0} \Omega_p^{[F:\mathbb{Q}]}$$

で定義する。

特にFが総実であるときには

$$r = r_1 - 1 = [F:\mathbb{Q}] - 1$$

であるから，§1と同様にしてFのp-進単数基準が±1倍を除いて定義される。

Leopoldt [5] はFが総実な$\mathbb{Q}$上のアーベル拡大である場合に類数公式のp-進化を構築し，これが無意味な等式ではないこと，即ちp-進単数基準が0でないことを予想した。

3. 単数群 $\mathcal{O}_F^\times$ を $\prod_{\mathfrak{p}|p} \mathcal{O}_{\mathfrak{p}}^\times$ にうめ込み，$\prod_{\mathfrak{p}|p}(1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}})$ に射影する写像を

$$\varphi : \mathcal{O}_F^\times \longrightarrow \prod_{\mathfrak{p}|p} (1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}})$$

としよう。この $\prod_{\mathfrak{p}|p}(1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}})$ には巾（の拡張）として$\mathbb{Z}_p$が作用し，$\mathbb{Z}_p$-加群の構造が入る。しかもこのとき $\lambda_0 \circ \log$ は$\mathbb{Z}_p$-加群としての準同型である。したがってFが総実なときには，Leopoldtの予想は $\varphi(\mathcal{O}_F^\times)$ の生成する $\prod_{\mathfrak{p}|p}(1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}})$ の$\mathbb{Z}_p$-部分加群の$\mathbb{Z}_p$上での essential rank が丁度 $r = r_1 - 1$ と一致する

ことと同値である。(ここで $(\lambda_0\cdot\log)^{-1}(0)$ は1の巾乗根で生成される有限群であることに留意されたい。) この $\varphi(\mathcal{O}_F^\times)$ が生成する $\mathbb{Z}_p$-加群は $\varphi(\mathcal{O}_F^\times)$ の閉包に他ならないことを注意しておこう。ここに一般の代数体Fに対してもLeopoldtの予想が次の命題としてとり出された:

$\varphi(\mathcal{O}_F^\times)$ の $\prod_{\mathfrak{p}|p}(1+\mathfrak{p}\mathcal{O}_\mathfrak{p})$ における閉包の $\mathbb{Z}_p$-加群としてのessential rankは $\mathcal{O}_F^\times$ の $\mathbb{Z}$-加群としてのessential rankと一致する。

II. $\mathbb{Z}_p$-拡大との関係

4. 代数体Fの $\mathbb{Z}_p$-拡大Kとは、Fのガロワ拡大でそのガロワ群 $Gal(K/F)$ が位相群として p-進整数の加法群 $\mathbb{Z}_p$ と同型になるものをいう。Leopoldtの予想とFの $\mathbb{Z}_p$-拡大との関係は、ヒルベルト理論のみから導びかれるが、ここでは類体論によってその関係を見ておく。

4-1. $\mathbb{Z}_p$-拡大KはFのアーベル拡大であり、F_{ab} をFの最大アーベル拡大とするとき F_{ab} の同型写像をKに制限することにより上への準同型写像 $\rho: Gal(F_{ab}/F)\longrightarrow Gal(K/F)$ が得られる。

一方Fのイデール群を$F_A^\times$とすれば，類体論のアルティン写像 $\alpha: F_A^\times \longrightarrow Gal(F_{ab}/F)$ は上への連続な開写像である。したがってFの$\mathbb{Z}_p$-拡大Kに対して上への連続準同型写像 $\xi: F_A^\times \longrightarrow \mathbb{Z}_p$ が

$$F_A^\times \xrightarrow{\alpha} Gal(F_{ab}/F) \xrightarrow{\rho} Gal(K/F) \cong \mathbb{Z}_p$$

によって得られる。そこで $X = \mathrm{Ker}\,\xi$ とすれば，この$F_A^\times$の閉部分群は

$$F_A^\times/X \cong \mathbb{Z}_p, \quad X \supset F^\# = \mathrm{Ker}\,\alpha$$

を満たす。ただし$F^\#$は，$F_A^\times$のアルキメデス的部分を$F_\infty^\times$，その1の連結成分を$F_{\infty+}^\times$とし，$F^\times$が$F_A^\times$に対角的にうめ込まれているとするときに，$F^\times \cdot F_{\infty+}^\times$ の$F_A^\times$における閉包と一致する。逆にこれらの条件を満たす$F_A^\times$の閉部分群Xが与えられれば，$\alpha(X)$が固定するF_{ab}の部分体としてFの$\mathbb{Z}_p$-拡大が得られる。

4-2. さて上の条件を満たすXに対しては，$F_\infty^\times \cdot X/X$ は，$F_A^\times/X \cong \mathbb{Z}_p$の有限部分群であり，よって$\mathbb{Z}_p$が有限部分群を有さぬから $X \supset F_\infty^\times$ がしたがう。そこで$F_A^\times$の非アルキメデス的部分を$F_0^\times$とするとき，$F_0^\times$の閉部分群Yで

$$F_0^\times/Y \cong \mathbb{Z}_p, \quad Y \supset F_0^\times \cap F^\#$$

を満たすものとXとは $X = Y \cdot F_\infty^\times$, $Y = X \cap F_0^\times$ によって完

全に対応している。

さらに $U=\prod_{\mathfrak{p}} \mathfrak{O}_{\mathfrak{p}}^{\times}\ (\subset F_0^{\times})$ とするとき，$F_0^{\times}/U\cdot(F_0^{\times}\cap F^{\#})$ は有限群である。したがって Y に対して $Z=Y\cap U$ をとれば，U/Z は $F_0^{\times}/Y\cong \mathbb{Z}_p$ の指数有限な閉部分群と見なせ，それ自身 $\mathbb{Z}_p$ の加法群と同型である。逆に U の閉部分群 Z で，

$$U/Z\cong \mathbb{Z}_p,\qquad Z\supset U\cap F^{\#}$$

を満たすものに対しては，$F_0^{\times}/Z\cdot(F_0^{\times}\cap F^{\#})$ のなかで位数が有限な元全体 T は有限群となり，$F_0^{\times}$ の閉部分群 Y を，自然な写像 $F_0^{\times}\longrightarrow F_0^{\times}/Z\cdot(F_0^{\times}\cap F^{\#})$ による T の逆像とすれば上の条件を満たす Y で $Z=Y\cap U$ となるものが唯一つ確定する。

4-3. 群 $U=\prod_{\mathfrak{p}} \mathfrak{O}_{\mathfrak{p}}^{\times}$ と $\mathbb{Z}_p$ は共に有限アーベル群の射影的極限となっており，有限アーベル群の Sylow 部分群の直積への唯一通りの分解は，そのまま U, $\mathbb{Z}_p$ に同様な分解をもたらす。特に p-群の極限としての $\mathbb{Z}_p$ は p-primary であるから，上の条件を満たす U の閉部分群 Z は，p と異なる素数 q に対しての U の q-primary な部分群をすべて含む。さて

$$\mathfrak{O}_{\mathfrak{p}}^{\times}=W_{\mathfrak{p}}\times(1+\mathfrak{p}\,\mathfrak{O}_{\mathfrak{p}}),$$

$$W_{\mathfrak{p}}=\{F_{\mathfrak{p}}\text{ の }(N_{F/\mathbb{Q}}(\mathfrak{p})-1)\text{ 乗根}\}$$

において，$W_{\mathfrak{p}}$ の Sylow p-部分群を $W_{\mathfrak{p}}^{(p)}$ とすれば，$\mathfrak{O}_{\mathfrak{p}}^{\times}$ の

最大の p-primary 部分群は

$$\begin{cases} \mathfrak{p}\nmid p \text{ ならば } W_{\mathfrak{p}}^{(p)} \\ \mathfrak{p}\mid p \text{ ならば } 1+\mathfrak{p}\mathfrak{O}_{\mathfrak{p}} \end{cases}$$

である。そこで

$$U^{(p)} = \prod_{\mathfrak{p}\nmid p} W_{\mathfrak{p}}^{(p)} \times \prod_{\mathfrak{p}\mid p}(1+\mathfrak{p}\mathfrak{O}_{\mathfrak{p}})$$

とすれば、上の条件を満たす U の閉部分群 Z はその最大の p-primary 部分群 $Z^{(p)} = Z \cap U^{(p)}$ によって決定される。したがって結局 $U^{(p)}$ の閉部分群 $Z^{(p)}$ であって

$$U^{(p)}/Z^{(p)} \cong \mathbb{Z}_p, \qquad Z^{(p)} \supset U^{(p)} \cap F^{\#}$$

となるものが問題となる。しかも $\mathbb{Z}_p$ の加法群が位数有限な元を 0 以外には有さない以上、各 $W_{\mathfrak{p}}^{(p)}$ $(\mathfrak{p}\nmid p)$ は $Z^{(p)}$ に含まれなければならない。よってさらにこれら位数有限な元を稠密に含む $\prod_{\mathfrak{p}\nmid p} W_{\mathfrak{p}}^{(p)}$ は $Z^{(p)}$ に含まれなければならない。

ここに F の $\mathbb{Z}_p$-拡大は次の条件を満たす $\prod_{\mathfrak{p}\mid p}(1+\mathfrak{p}\mathfrak{O}_{\mathfrak{p}})$ の閉部分群 R と完全に対応づけられた:

$$\prod_{\mathfrak{p}\mid p}(1+\mathfrak{p}\mathfrak{O}_{\mathfrak{p}})/R \cong \mathbb{Z}_p,$$
$$R \supset \prod_{\mathfrak{p}\mid p}(1+\mathfrak{p}\mathfrak{O}_{\mathfrak{p}}) \cap F^{\#}。$$

4-4. 最後に $F^{\#}$ に関する部分をしらべよう。

よく知られているように、$F^{\#}$ は $F_A^{\times}$ における $F^{\times} F_{\infty+}^{\times}$ の閉包であった。さて $[F^{\#} F_{\infty}^{\times} : F^{\#}] < \infty$ であるから、$F^{\#} F_{\infty}^{\times}$

は$F_A^\times$の閉集合であり，よって$F^\times\cdot F_\infty^\times$の閉包$\overline{F^\times\cdot F_\infty^\times}$である。上の$R$についての条件において$F^\#$に関する部分は$F^\#$を$\overline{F^\times F_\infty^\times}$でおきかえてよいことは明らかである。さらにいま$x \in F_A^\times$を$\overline{F^\times\cdot F_\infty^\times}$の元とするとき，$U\cdot F_\infty^\times$が$F_A^\times$の開部分群であるから，適当に$a \in F^\times$, $b \in F_\infty^\times$を選べば$xa^{-1}b^{-1} \in U$とすることができる。また$U \cap F^\times F_\infty^\times$は$\mathfrak{O}_F^\times$の$F_A^\times$の非アルキメデス的部分$F_0^\times$への射影$(\mathfrak{O}_F^\times)_0$にほかならない。そこで$(\mathfrak{O}_F^\times)_0$の閉包を$\overline{(\mathfrak{O}_F^\times)_0}$とするとき，

$$\overline{F^\times\cdot F_\infty^\times} = \overline{(\mathfrak{O}_F^\times)_0}\cdot F^\times\cdot F_\infty^\times$$

であることは見易い。よって明らかに

$$U \cap \overline{F^\times\cdot F_\infty^\times} = \overline{(\mathfrak{O}_F^\times)_0}$$

である。すでに見たように$\prod_{\mathfrak{p}|p}(1+\mathfrak{p}\mathfrak{O}_\mathfrak{p})$は$U$の直積因子であった。そこで$\varphi: \mathfrak{O}_F^\times \longrightarrow \prod_{\mathfrak{p}|p}(1+\mathfrak{p}\mathfrak{O}_\mathfrak{p})$をI-§3の写像とすれば，$\prod_{\mathfrak{p}|p}(1+\mathfrak{p}\mathfrak{O}_\mathfrak{p}) \cap \overline{(\mathfrak{O}_F^\times)_0}$は$\varphi(\mathfrak{O}_F^\times)$の閉包$\overline{\varphi(\mathfrak{O}_F^\times)}$にほかならない。

また$\mathbb{Z}_p$-加群としての$\prod_{\mathfrak{p}|p}(1+\mathfrak{p}\mathfrak{O}_\mathfrak{p})$の essential rank は$[F:\mathbb{Q}] = r_1 + 2\cdot r_2$であった。ここに次の定理が示された：

<u>定理 1.</u> 類体論によってFの$\mathbb{Z}_p$-拡大は$\prod_{\mathfrak{p}|p}(1+\mathfrak{p}\mathfrak{O}_\mathfrak{p})$の閉部分群$R$で

$$\prod_{\mathfrak{p}|p}(1+\mathfrak{p}\mathfrak{O}_\mathfrak{p})/R \cong \mathbb{Z}_p, \qquad R \supset \varphi(\mathfrak{O}_F^\times)$$

を満たすものと完全に対応する。したがって特にFの$\mathbb{Z}_p$-拡大のなかで独立なものの最大個数は

$$[F:\mathbb{Q}] - \mathrm{ess.rank}_{\mathbb{Z}_p} \overline{\varphi(\mathcal{O}_F^{\times})} \geqq r_2 + 1$$

であり，等号が成立することと，Fのpに関するLeopoldtの予想が正しいことが同値である。

注意 Chevalley [3] からは $\overline{(\mathcal{O}_F^{\times})}_{\circ} \cap U^{(p)}$ の$\mathbb{Z}_p$上のess. rankが$r = r_1 + r_2 - 1$に等しいことが容易に導びかれる。

III. Ax-Brumerの方法の拡張

5. 代数体Fの自己同型群を$G = \mathrm{Aut}(F)$とする。準同型写像$\varphi : \mathcal{O}_F^{\times} \longrightarrow \prod_{\mathfrak{p}|p} (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}})$は$\mathbb{Z}[G]$-加群としての準同型であり，特に$E \cap \mathrm{Ker}\,\varphi = \{1\}$である。ただし$\mathbb{Z}[G]$は$\mathbb{Z}$上の有限群$G$の群環である。

さて$\mathbb{Z}$上あるいは$\mathbb{Z}_p$上の加群のessential ranksを問題にする限り，$\underset{\mathbb{Z}}{\otimes}\mathbb{Q}$をほどこしてベクトル空間の次元を考察するほうが簡明である。そこで

$$V = \mathcal{O}_F^{\times} \underset{\mathbb{Z}}{\otimes} \mathbb{Q} = E \underset{\mathbb{Z}}{\otimes} \mathbb{Q},$$

$$V' = \Big(\prod_{\mathfrak{p}|p} (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}})\Big) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$$

とおくとき，Vは$\mathbb{Q}$上のr次元ベクトル空間であり，一方V'は自然に$\mathbb{Q}_p=\mathbb{Z}_p\underset{\mathbb{Z}}{\otimes}\mathbb{Q}$上のベクトル空間と見される。また$\dim_{\mathbb{Q}_p}V'=[F:\mathbb{Q}]$である。上の$\varphi$は$\mathbb{Q}[G]$-準同型

$$\Phi : V \longrightarrow V'$$

を与え，$\mathrm{Ker}\,\Phi=\{0\}$である。さて

$$\text{Leopoldt の予想} \iff \dim_{\mathbb{Q}_p}(\mathbb{Q}_p\cdot\Phi(V))=r$$

であるから，Φを$\mathbb{Q}_p$上の線型写像

$$\Phi_p : V\underset{\mathbb{Q}}{\otimes}\mathbb{Q}_p \longrightarrow V'$$

に拡張しておけば，これは$\mathbb{Q}_p[G]$-準同型であり，次の命題を得る。

<u>命題 1.</u> 素数pに関して，Leopoldtの予想はΦ_pが$1:1$であることと同値である。

<u>注意</u> $\Phi_p|_V=\Phi$は$1:1$である。

6. このΦ_pは$\mathbb{Q}_p[G]$-準同型であるから$\mathrm{Ker}\,\Phi_p$は$\mathbb{Q}_p[G]$-不変である。有限群Gの$\mathbb{Q}_p$上の表現は完全可約であるから$V\otimes\mathbb{Q}_p$の$\mathbb{Q}_p[G]$-部分空間Xであって

$$V\otimes\mathbb{Q}_p = X\oplus\mathrm{Ker}\,\Phi_p$$

となるものが存在する。そこで

$$\pi : V \otimes \mathbb{Q}_p \longrightarrow \operatorname{Ker} \Phi_p$$

をこの直和分解による射影とすれば，π は $\mathbb{Q}_p[G]$-準同型である。

$G = \operatorname{Aut}(F)$ の $V = \mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Q}$ 上での表現を

$$\rho : G \longrightarrow \operatorname{End}_{\mathbb{Q}}(V)$$

とし，これから得られる G の $V \otimes_{\mathbb{Q}} \mathbb{Q}_p$ 上での表現を

$$\rho_p : G \longrightarrow \operatorname{End}_{\mathbb{Q}_p}(V \otimes \mathbb{Q}_p)$$

とすれば，これらは多元環の準同型

$$\rho : \mathbb{Q}[G] \longrightarrow \operatorname{End}_{\mathbb{Q}}(V),$$

$$\rho_p : \mathbb{Q}_p[G] \longrightarrow \operatorname{End}_{\mathbb{Q}_p}(V \otimes \mathbb{Q}_p)$$

をひきおこす。$\operatorname{End}_{\mathbb{Q}}(V)$ 内での $\rho(\mathbb{Q}[G])$ の可換子環を

$$\widetilde{\rho(\mathbb{Q}[G])} = \{ x \in \operatorname{End}_{\mathbb{Q}}(V) \mid \forall y \in \rho(\mathbb{Q}[G]) \, (x \circ y = y \circ x) \}$$

とすれば，$\operatorname{End}_{\mathbb{Q}_p}(V \otimes \mathbb{Q}_p)$ での $\rho_p(\mathbb{Q}_p[G])$ の可換子環は

$$\widetilde{\rho_p(\mathbb{Q}_p[G])} = \widetilde{\rho(\mathbb{Q}[G])} \otimes_{\mathbb{Q}} \mathbb{Q}_p$$

で与えられる。

さて上の $\pi : V \otimes \mathbb{Q}_p \longrightarrow \operatorname{Ker} \Phi_p$ を

$$V \otimes \mathbb{Q}_p \longrightarrow \operatorname{Ker} \Phi_p \hookrightarrow V \otimes \mathbb{Q}_p$$

と見れば $\pi \in \operatorname{End}_{\mathbb{Q}_p}(V \otimes \mathbb{Q}_p)$ であって

(1) $\pi \circ \pi = \pi$,

(2) $\forall g \in G \, (\pi \circ \rho(g) = \rho(g) \circ \pi)$

となっている。

命題2. 射影 $\pi: V\otimes\mathbb{Q}_p \longrightarrow \mathrm{Ker}\,\Phi_p$ を $\mathrm{End}_{\mathbb{Q}_p}(V\otimes\mathbb{Q}_p)$ の元と見なしたとき，π は $\rho_p(\mathbb{Q}_p[G])$ に属する巾等元である。

Leopoldt の予想は $\pi=0$ と同値である。

7. この節では Brumer [2] の超越的結果の応用を行う。

§2 と同様に，Ω_p を $\mathbb{Q}_p$ の代数的閉包の完備化とし，その附値を $|\cdot|_p$ と表わそう。$\{u\in\Omega_p \mid |u|_p\leq 1\}=\mathcal{O}_{\Omega_p}$ は Ω_p の整数環であり，この正則元全体 $\mathcal{O}_{\Omega_p}^{\times}$ が Ω_p の単数のなす群である。さて p-進対数関数

$$\log x = -\sum_{n=1}^{\infty}\frac{1}{n}\cdot(1-x)^n$$

は $|1-x|_p<1$ なる $x\in\mathcal{O}_{\Omega_p}^{\times}$ に対して定義されて Ω_p の数に収束する。さらに 1 の巾乗根 $\zeta\in\mathcal{O}_{\Omega_p}^{\times}$ に対しては $\log\zeta=0$ とすることにより，$\log x$ は $\mathcal{O}_{\Omega_p}^{\times}$ 上の関数と見なせ，$\log(x\cdot y)=\log x+\log y\ (x,y\in\mathcal{O}_{\Omega_p}^{\times})$ が成り立っている。

<u>Brumer の定理</u>　単数 $u_1,\cdots,u_n\in\mathcal{O}_{\Omega_p}^{\times}$ が $\mathbb{Q}$ 上代数的であるとする。もし $\log u_1,\cdots,\log u_n\in\Omega_p$ が $\mathbb{Q}$ 上一次独立であるならば，これらは Ω_p における $\mathbb{Q}$ の代数的閉包上でも一次独立である。

この定理に帰着させて次の定理を証明する。これは§6のπについて，$\pi \neq 0$（即ち $\mathrm{Ker}\,\Phi_p \neq \{0\}$）であるとすれば，$\pi$（あるいは $\mathrm{Ker}\,\Phi_p$）は'超越的'であることを主張する。

体$\mathbb{Q}_p$における$\mathbb{Q}$の代数的閉包をAとしよう。

定理 2. $\{\pi\circ\psi \mid \psi \in \mathrm{End}_{\mathbb{Q}_p}(V \otimes_{\mathbb{Q}} \mathbb{Q}_p)\} \cap \mathrm{End}_A(V \otimes_{\mathbb{Q}} A) = \{0\}$.

証明　ある $\psi \in \mathrm{End}_{\mathbb{Q}_p}(V \otimes_{\mathbb{Q}} \mathbb{Q}_p)$ に対して $\pi\circ\psi \in \mathrm{End}_A(V \otimes_{\mathbb{Q}} A)$ であるとしよう。自然に $\mathrm{End}_A(V \otimes_{\mathbb{Q}} A) = \mathrm{End}_{\mathbb{Q}}(V) \otimes_{\mathbb{Q}} A$ と見なせるから

$$\pi\circ\psi = a_1\cdot\alpha_1 + \cdots + a_t\cdot\alpha_t$$

$$\alpha_1, \cdots, \alpha_t \in \mathrm{End}_{\mathbb{Q}}(V);\quad a_1, \cdots, a_t \in A$$

とあらわされる。さて $\mathcal{O}_F^\times = W_F \times E$ においてEの$\mathbb{Z}$上の生成元 $\varepsilon_1, \cdots, \varepsilon_r$ をとるとき

$$\mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Q} = V = \mathbb{Q}\cdot\varepsilon_1 + \cdots + \mathbb{Q}\cdot\varepsilon_r$$

である。ただしVにおいては加法的に記すことにする。また $\dim_{\mathbb{Q}} V = r$，即ち $\varepsilon_1, \cdots, \varepsilon_r$ は$\mathbb{Q}$上一次独立である。

さて $\pi\circ\psi \neq 0$ と仮定しよう。このときある $\varepsilon \in E$ に対して $\pi\circ\psi(\varepsilon) \neq 0$ である。このεに注目してBrumerの定理と矛盾が生じることを示す。各 α_j $(1 \leq j \leq t)$ は $\mathrm{End}_{\mathbb{Q}}(V)$ の元であるから，

$$\alpha_j(\varepsilon) = d_{j1}\cdot\varepsilon_1 + \cdots + d_{jr}\cdot\varepsilon_r$$
$$d_{j1}, \cdots, d_{jr} \in \mathbb{Q}$$

と表わされる。したがって

$$\pi\circ\psi(\varepsilon) = b_1\cdot\varepsilon_1 + \cdots + b_r\cdot\varepsilon_r$$
$$b_\mu = d_{1\mu}\cdot a_1 + \cdots + d_{t\mu}\cdot a_\mu \in A$$
$$(\mu = 1, \cdots, r)$$

であり，特に $\pi\circ\psi(\varepsilon) \neq 0$ であるから，ある μ に対しては，$b_\mu \neq 0$ である。一方 $\pi\circ\psi(\varepsilon) \in \mathrm{Ker}\,\Phi_p$ である。よって

$$b_1\cdot\Phi_p(\varepsilon_1) + \cdots + b_r\cdot\Phi_p(\varepsilon_r) = 0$$
$$b_1, \cdots, b_r \in A;\ \text{ある } b_\mu \neq 0$$

となっている。ここに

$$\Phi_p : V\otimes\mathbb{Q}_p = \mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p \longrightarrow V' = \Big(\prod_{\mathfrak{p}|p}(1+\mathfrak{p}\mathcal{O}_\mathfrak{p})\Big)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$$

はうめ込み写像 $\mathcal{O}_F^\times \hookrightarrow \prod_{\mathfrak{p}|p}\mathcal{O}_\mathfrak{p}^\times$ から得られた。さて p-進対数関数による $\log : \prod_{\mathfrak{p}|p}\mathcal{O}_\mathfrak{p}^\times \longrightarrow \bigoplus_{\mathfrak{p}|p}F_\mathfrak{p}$ は $\mathbb{Z}_p$-加群としての準同型であり，自然に $\mathbb{Q}_p$ 上の線型写像 $\log : V' \longrightarrow \bigoplus_{\mathfrak{p}|p}F_\mathfrak{p}$ に拡張できる。また §2 で述べたうめ込み

$$\lambda_0 : \bigoplus_{\mathfrak{p}|p}F_\mathfrak{p} = F\otimes_{\mathbb{Q}}\mathbb{Q}_p \longrightarrow F\otimes_{\mathbb{Q}}\Omega_p \cong \Omega_p^{[F:\mathbb{Q}]}$$

はやはり $\mathbb{Q}_p$ 上の線型写像である。したがって

$$\lambda_0\circ\log : V' \longrightarrow \Omega_p^{[F:\mathbb{Q}]}$$

は $\mathbb{Q}_p$ 上線型である。そこで $\Psi = \lambda_0\circ\log\circ\Phi_p$ とおくとき，$\Omega^{[F:\mathbb{Q}]}$ のベクトル $\Psi(\varepsilon_1), \cdots, \Psi(\varepsilon_r)$ は

$$b_1\cdot\Phi(\varepsilon_1)+\cdots+b_r\cdot\Phi(\varepsilon_r)=0$$

$$b_1,\cdots,b_r\in A;\quad \text{ある } b_\mu\neq 0$$

なる関係を有する。そこで例えば、それらのベクトルの第一座標に注目すれば、あるうめ込み $\sigma: F\longrightarrow\Omega_p$ に対して

$$b_1\log(\sigma(\varepsilon_1))+\cdots+b_r\cdot\log(\sigma(\varepsilon_r))=0$$

$$b_1,\cdots,b_r\in A;\quad \text{ある } b_\mu\neq 0$$

となっている。これは $\varepsilon_1,\cdots,\varepsilon_r$ のとり方から Brumer の定理と矛盾する。証明終り。

<u>注意</u>　§6, 7 の議論はそのまま次の形に一般化される。

単数群 $\mathcal{O}_F^\times$ の部分群 E_1 に対して $V_1=E_1\otimes_{\mathbb{Z}}\mathbb{Q}$ とすれば、V_1 は $V=\mathcal{O}_F^\times\otimes_{\mathbb{Z}}\mathbb{Q}$ の部分空間になっている。さて $\mathrm{Aut}(F)$ の部分群 G_1 で条件

$$\forall g\in G_1\ (g(W_F\cdot E_1)\subset W_F\cdot E_1)$$

を満たすものをとるとき、V_1 は自然に G_1-加群になる。そこで $V_1\otimes_{\mathbb{Q}}\mathbb{Q}_p$ を $V\otimes\mathbb{Q}_p$ の部分空間とみなせば、

$$V_1\otimes\mathbb{Q}_p=X_1\oplus(\mathrm{Ker}\,\Phi_p\cap V_1\otimes\mathbb{Q}_p)$$

なる形に G_1-加群としての直和に分解される。この分解による射影 $\pi_1: V_1\otimes\mathbb{Q}_p\longrightarrow\mathrm{Ker}\,\Phi_p\cap V_1\otimes\mathbb{Q}_p$ を $\mathrm{End}_{\mathbb{Q}_p}(V_1\otimes\mathbb{Q}_p)$ の元と見なし、また G_1 の $V_1\otimes\mathbb{Q}_p$ 上での表現を $\rho_{1,p}$、またさらに $\mathrm{End}_{\mathbb{Q}_p}(V_1\otimes\mathbb{Q}_p)$ での $\rho_{1,p}(\mathbb{Q}_p[G_1])$ の可換子を $\widetilde{\rho_{1,p}(\mathbb{Q}_p[G_1])}$

とすれば、次を得る。

<u>命題</u>　π_1 は $\rho_{1,p}(\widetilde{\mathbb{Q}_p[G_1]})$ の巾等元である。

<u>定理</u>　$\{\pi_1 \circ \psi \mid \psi \in \mathrm{End}_{\mathbb{Q}_p}(V_1 \otimes_{\mathbb{Q}} \mathbb{Q}_p)\} \cap \mathrm{End}_A(V_1 \otimes_{\mathbb{Q}} A) = \{0\}$。

IV　虚２次体のガロワ拡大体の場合

代数体 F をある虚２次体 k のガロワ拡大体とし、$\mathrm{Aut}(F)$ の部分群 $G = \mathrm{Gal}(F/k)$ をとる。この場合には $r_1 = 0$, $r_2 = [F:k]$, $r = [F:k] - 1$ となっている。

8.　この節では §6 の環 $\rho(\mathbb{Q}[G]) \subset \mathrm{End}_{\mathbb{Q}}(V)$ と $\rho(\widetilde{\mathbb{Q}[G]})$ との構造を明らかにする。

Herbrand [4] は、G の V 上での表現 ρ と自明な表現 1 との直和 $\rho \oplus 1$ が G の正則表現と同値であることを指摘した。したがって次を得る。

<u>命題 3</u>. 群 G が $\mathbb{Q}$ 上に自明に作用するとき、左 $\mathbb{Q}[G]$-加群 $V \oplus \mathbb{Q}$ は、$\mathbb{Q}$ 上の G の群環 $\mathbb{Q}[G]$ を自然に左 $\mathbb{Q}[G]$-加群と見

たときにこれと $\mathbb{Q}[G]$-同型である。

<u>定理 3</u> 環 $\rho(\mathbb{Q}[G])$ と $\widetilde{\rho(\mathbb{Q}[G])}$ とは同型であり、しかも環としての直和 $\rho(\mathbb{Q}[G])\oplus\mathbb{Q}\cong\widetilde{\rho(\mathbb{Q}[G])}\oplus\mathbb{Q}$ は群環 $\mathbb{Q}[G]$ と同型である。

<u>証明</u> 命題3により $V\oplus\mathbb{Q}=\mathbb{Q}[G]$ と見なし $\rho(\mathbb{Q}[G])\oplus\mathbb{Q}=\mathbb{Q}[G]$ が左から作用するとする。さて $\mathbb{Q}[G]=B_0\oplus\cdots\oplus B_s$ を半単純環 $\mathbb{Q}[G]$ の単純部分環 B_j $(j=0,1,\cdots,s)$ の直和への分解とし、各 B_j の中心を C_j, 単位元を e_j とする。これら C_j は $\mathbb{Q}$ 上の有限次元代数的拡大体であり、B_j は C_j 上の中心的単純環である。さて $\mathrm{End}_{\mathbb{Q}}(V\oplus\mathbb{Q})$ における $\mathbb{Q}[G]=\rho(\mathbb{Q}[G])\oplus\mathbb{Q}$ の可換子環を D とするとき、D の各元は $V\oplus\mathbb{Q}$ の $\mathbb{Q}[G]$-部分空間 $e_j(V\oplus\mathbb{Q})$ を不変にする。したがって $\mathrm{End}_{\mathbb{Q}}(e_j(V\oplus\mathbb{Q}))$ における B_j の可換子環を D_j $(j=0,1,\cdots,s)$ とするとき、$\mathbb{Q}[G]=B_0\oplus\cdots\oplus B_s$ に対応して $D=D_0\oplus\cdots\oplus D_s$ となる。左 B_j-加群 $V_j=e_j(V\oplus\mathbb{Q})=e_j(\mathbb{Q}[G])$ は左 B_j-加群としての B_j 自身である。さらに V_j に左から作用する B_j の $\mathrm{End}_{\mathbb{Q}}(V_j)$ における可換子環 D_j は B_j の中心 C_j を含み、B_j も D_j も共に $\mathrm{End}_{C_j}(V_j)$ に含まれている。しかも D_j はこの $\mathrm{End}_{C_j}(V_j)$ における B_j の可換子環になっている。一方 C_j のベクトル空間と

見た $V_j = B_j$ には，右から B_j が自然に作用し，明らかにこれは左からの B_j の作用と可換である。この右からの B_j の作用は，B_j の inverse algebra を B_j^* とするとき，B_j^* の左からの作用と見てよい。このとき B_j の中心 C_j はそのまま B_j^* に含まれているとしてよく，結局 C_j 上の単純環 $B_j \otimes_{C_j} B_j^*$ から $\mathrm{End}_{C_j}(V_j)$ に自然に準同型 η が定義され，$B_j^* = e_j \otimes B_j^*$ の像は D_j に含まれている。しかも $B_j \otimes_{C_j} B_j^*$ は単純であるから，この η は1対1であり，さらに C_j 上のベクトル空間としての次元をくらべれば

$$
\begin{aligned}
[B_j : C_j]^2 = [B_j : C_j]\cdot[B_j^* : C_j] &= [B_j \otimes_{C_j} B_j^* : C_j] \\
&= [\eta(B_j \otimes_{C_j} B_j^*) : C_j] \\
&\leqq [\mathrm{End}_{C_j}(V_j) : C_j] = [B_j : C_j]^2
\end{aligned}
$$

を得る。よって等号が成り立ち $\eta(B_j \otimes B_j^*) = \mathrm{End}_{C_j}(V_j)$ である。したがって $\eta(B_j^*) = D_j$。ここに $V \oplus \mathbb{Q} = \mathbb{Q}[G]$ に左から作用する $\mathbb{Q}[G]$ の $\mathrm{End}_{\mathbb{Q}}(V \oplus \mathbb{Q})$ における可換子環は，右から作用する $\mathbb{Q}[G]$，即ち左から作用する $\mathbb{Q}[G]$ の inverse algebra $\mathbb{Q}[G]^*$ であることが示された。一方

$$
\mathbb{Q}[G] \ni \sum_{g \in G} a_g \cdot g \longmapsto \sum_{g \in G} a_g \cdot g^{-1} \in \mathbb{Q}[G]
$$

は $\mathbb{Q}[G]$ と $\mathbb{Q}[G]^*$ との $\mathbb{Q}$ 上の多元環としての同型を与える。ここに $\rho(\mathbb{Q}[G]) \oplus \mathbb{Q} = \mathbb{Q}[G] \cong \mathbb{Q}[G]^* = \widetilde{\rho(\mathbb{Q}[G])} \oplus \mathbb{Q}$ が示された。この同型は直和を保っており，$\rho(\mathbb{Q}[G])$ と $\widetilde{\rho(\mathbb{Q}[G])}$

との環としての同型を導びくことも明らかであろう。証明終り。

注意　この $\mathbb{Q}[G]$ と $\mathbb{Q}[G]^*$ との同型は，各 j に対して B_j と B_j^* との同型を与える。しかしこの B_j と B_j^* との同型はあくまでも $\mathbb{Q}$ 上の多元環としての同型であり，一般には中心 C_j 上の同型，即ち C_j 上で恒等的になるとは限らない。

9.　この節では $\rho_p(\widetilde{\mathbb{Q}_p[G]}) = \rho(\widetilde{\mathbb{Q}[G]}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ の中心に属する巾等元がすべて'$\mathbb{Q}$ 上代数的'であることを示し，次の節で $\rho_p(\widetilde{\mathbb{Q}_p[G]})$ の巾等元がすべて中心に属するような群 G と素数 p との組み合わせを決定する。

§7 と同様に A を $\mathbb{Q}$ の $\mathbb{Q}_p$ における代数的閉包としよう。

命題4　$\rho_p(\widetilde{\mathbb{Q}_p[G]}) = \rho(\widetilde{\mathbb{Q}[G]}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ の巾等元がその中心に属するならば，実は $\rho(\widetilde{\mathbb{Q}[G]}) \otimes_{\mathbb{Q}} A$ に属する。

証明　$\rho(\widetilde{\mathbb{Q}[G]}) = D_1 \oplus \cdots \oplus D_s$ を単純部分環 D_j $(j=1,\cdots,s)$ による直和分解とし，C_j を D_j の中心とする。このとき $C = C_1 \oplus \cdots \oplus C_s$ は $\rho(\widetilde{\mathbb{Q}[G]})$ の中心であり，$\rho_p(\widetilde{\mathbb{Q}_p[G]})$ の中心

は $C\otimes_{\mathbb{Q}}\mathbb{Q}_p$ である。しかも $C\otimes\mathbb{Q}_p$ の巾等元は $C_j\otimes_{\mathbb{Q}}\mathbb{Q}_p$ ($j=1,\cdots,s$) の巾等元の和として得られるから、各 C_j について $C_j\otimes_{\mathbb{Q}}\mathbb{Q}_p$ の巾等元がすべて $C_j\otimes_{\mathbb{Q}}A$ に属することを示せば十分であろう。そこで

C を $\mathbb{Q}$ の有限次代数的拡大体とするとき、$C\otimes_{\mathbb{Q}}\mathbb{Q}_p$ の巾等元が $C\otimes_{\mathbb{Q}}A$ に属する

ことを示す。まず Ω_p での $\mathbb{Q}$ の代数的閉包を $\overline{\mathbb{Q}}$ とすれば、$A=\overline{\mathbb{Q}}\cap\mathbb{Q}_p$ である。一方 $C=\mathbb{Q}(\alpha)$ ($\alpha\in C$) として、α を根にもつ $\mathbb{Q}$ 係数の既約多項式を $P(X)\in\mathbb{Q}[X]$ とすれば、C は自然に剰余体 $\mathbb{Q}[X]/P\cdot\mathbb{Q}[X]$ と同型になる。さて $\mathbb{Q}_p[X]$ において $P(X)=P_1(X)\cdots P_t(X)$ と既約多項式 $P_\nu(X)\in\mathbb{Q}_p[X]$ の積に分解されたとしよう。このとき定数倍で修正して、各 $P_\nu(X)$ が $\overline{\mathbb{Q}}[X]$ の一次式の積になっているとしてよい。即ち各 $P_\nu(X)$ は $A[X]$ に属するとしてよい。しからば

$$C\otimes_{\mathbb{Q}}A\cong A[X]/P_1\cdot A[X]\oplus\cdots\oplus A[X]/P_t\cdot A[X]$$

と分解され、各 $A[X]/P_\nu\cdot A[X]$ は体である。その単位元と対応する $C\otimes A$ の元を e_ν ($\nu=1,\cdots,t$) とすれば、$C\otimes A$ の巾等元は(0 と)いくつかの e_ν の和でつくされる。しかも各 $P_\nu(X)$ が $\mathbb{Q}_p[X]$ でも既約であることから、各 $\mathbb{Q}_p[X]/P_\nu\cdot\mathbb{Q}[X]$ は体であり、したがって $C\otimes_{\mathbb{Q}}\mathbb{Q}_p$ の巾等元はすべて $C\otimes_{\mathbb{Q}}A$ に含まれている。証明終り。

注意　この証明はかなり一般的な場合にそのままあてはまる。例えばBを完全体K上の準単純な多元環とし，MをKを含む体，MにおけるKの代数的閉包をLとすれば，$B\otimes_K M$ の巾等元がその中心に属するとき，それは $B\otimes_K L$ に属する。

10. さて $\rho_p\widetilde{(\mathbb{Q}_p[G])} = \rho\widetilde{(\mathbb{Q}[G])}\otimes_{\mathbb{Q}} \mathbb{Q}_p$ の巾等元がことごとく $\rho\widetilde{(\mathbb{Q}[G])}\otimes_{\mathbb{Q}} A$ に属することと，$\mathbb{Q}[G] = \rho\widetilde{(\mathbb{Q}[G])}\oplus \mathbb{Q}$ について，$\mathbb{Q}_p[G]$ の巾等元がすべて $A[G]$ に属することとは同値である。そこで有限群Gに対して $\mathbb{Q}_p[G]$ の巾等元がすべて中心に属する場合を決定しよう。

命題5　可換体M上の準単純な多元環Bにおいて，Bの巾等元がすべて中心に含まれるための必要かつ十分な条件は，Bが斜体（可換体であってもよい）の直和になっていることである。

証明　M上の単純環 $B_1,\cdots,B_t$ によって $B=B_1\oplus\cdots\oplus B_t$ と分解されたとき，各 B_ν はある斜体 D_ν 上の正方行列環 $M_{n_\nu}(D_\nu)$ と同型である。Bの巾等元は B_ν の巾等元の和として表わされる。したがってもしある $n_\nu>1$ ならば明らか

に $M_{n_\nu}(M)$ $(\subset M_{n_\nu}(D_\nu))$ には中心に属さない巾等元が存在するし，逆に $n_\nu = 1$ $(\nu = 1, \cdots, t)$ であるならば $B_\nu = D_\nu$ の巾等元は0か単位元しかなく，したがって B の巾等元はすべて中心に属する。証明終り。

命題6　体Mの標数が有限群 G の位数 $|G|$ と素なとき，群環 $M[G]$ の巾等元がすべてその中心に属するならば，G の部分群はすべて正規部分群である。

証明　G_1 を G の部分群とし $\iota = \frac{1}{|G_1|} \cdot \sum_{g_1 \in G_1} g_1 \in M[G]$ を考えよう。このとき $\iota^2 = \iota$ は見易い。よって ι は $M[G]$ の巾等元であり，中心に属する。したがってどの $g \in G$ に対しても $g^{-1} \cdot \iota \cdot g = \iota$ であり，これは G_1 が G の正規部分群であることを示す。証明終り。

(1) 群 G がアーベル群であれば，明らかにすべての p に対して $\mathbb{Q}_p[G]$ の巾等元は中心に属している。

(2) 群 G はアーベル群でないとしよう。ある p に対して $\mathbb{Q}_p[G]$ の巾等元がすべてその中心に属しているとする。このとき命題6より G はハミルトン群でなければならない。よって G は位数8の quaternion 群 G_1 と，exponent がある奇数 m

に対して m または $2m$ であるアーベル群 G_2 との直積でなければならない。したがって，$\mathbb{Q}$ 上の四元数環 H を

$$H = \{a + b\cdot i + c\cdot j + d\cdot k \mid a, b, c, d \in \mathbb{Q}\}$$

$$i^2 = j^2 = -1; \quad ij = -ji = k$$

とし，$\nu | m$ なる ν に対して 1 の原始 ν 乗根のひとつを ζ_ν とするとき，$\mathbb{Q}_p[G]$ の単純環への直和分解にあらわれる非可換環は $H \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_p(\zeta_\nu)$ $(\nu | m)$ でつくされる。よく知られているように

(イ) $p \neq 2$ なら $H \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$ であり，

(ロ) $p = 2$ のときは，$H \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_2(\zeta_\nu)$ が斜体であるための必要十分条件は $[\mathbb{Q}_2(\zeta_\nu) : \mathbb{Q}_2]$ が奇数であることである。また $\nu | m$ ならば $\mathbb{Q}_2(\zeta_\nu) \subset \mathbb{Q}_2(\zeta_m)$ となっている。よって $d = [\mathbb{Q}_2(\zeta_m) : \mathbb{Q}_2]$ が奇数であるならば，各 $\nu | m$ に対して $[\mathbb{Q}_2(\zeta_\nu) : \mathbb{Q}_2]$ も奇数になる。さて m は奇数であるから $\mathbb{Q}_2(\zeta_m) / \mathbb{Q}_2$ は不分岐で，$\mathbb{Q}_2(\zeta_m)$ に含まれる 1 の巾乗根は $2\cdot(2^d - 1)$ 乗根の全体と一致する。よって $m | 2^d - 1$。また奇数 d_1 に対して $m | 2^{d_1} - 1$ とするとき，$\mathbb{Q}_2$ の不分岐な d_1 次拡大体 K をとれば，K には 1 の $(2^{d_1} - 1)$ 乗根がすべて含まれ，したがって $\mathbb{Q}_2(\zeta_m) \subset K$。よって $d = [\mathbb{Q}_2(\zeta_m) : \mathbb{Q}_2]$ は奇数 d_1 の約数であってそれ自身奇数である。

以上をまとめて

命題7　有限群Gと素数pに対して群環$\mathbb{Q}_p[G]$の巾等元がすべて中心に含まれるのは次の場合であり，またこれにつきる。

(1)　アーベル群Gとすべてのp；

(2)　$p=2$，　$G=G_1\times G_2$：

$$\begin{cases} G_1=\langle a,b\rangle : a^4=1,\ a^2=b^2,\ b^{-1}ab=a^{-1}; \\ G_2 : \text{アーベル群でその exponent が，} m \mid 2^{2\mu+1}-1 \\ \quad (\mu\in\mathbb{N})\text{ なる } m \text{ に対して，} m \text{ 又は } 2m \text{ のもの。} \end{cases}$$

さて命題2，定理2，3，命題4，7をあわせれば，直に次の定理を得る。

定理（Ax－Brumer）　虚2次体のアーベル拡大体に含まれる代数体については，すべてのpに対してLeopoldtの予想が正しい。

定理4　虚2次体のガロワ拡大体で，そのガロワ群が命題7，(2)の群と同型であるものの部分体については，$p=2$に対してLeopoldtの予想が正しい。

注意　§7の最後の注意で述べた命題，定理と例えば命題4

とを組み合わせれば次の結果を得る：

一般に F を有限次代数体とし $\mathcal{O}_F^\times$ の部分群 E_1 と $\mathrm{Aut}(F)$ の部分群 G_1 が §7 最後の注意にある条件を満たしているとする。さらに，G_1 の $V_1 = E_1 \otimes_{\mathbb{Z}} \mathbb{Q}$ 上の表現 ρ_1 が条件：

ρ_1 に含まれる絶対既約な G_1 の表現の重複度はすべて 1 である，

を満たすならば $\mathrm{End}_{\mathbb{Q}}(V_1)$ における $\rho_1(\mathbb{Q}[G])$ の可換子環たる $\widetilde{\rho_1(\mathbb{Q}[G])}$ は可換体の直和であり，したがって $\widetilde{\rho_{1,p}(\mathbb{Q}_p[G])}$ は可換環である。よってこのとき

<u>定理</u> $\quad \mathrm{ess.rank}_{\mathbb{Z}} E_1 = \mathrm{ess.rank}_{\mathbb{Z}_p} \overline{\varphi(E_1)}$

がすべての p に対して成立する。

11. この節では，虚２次体 k 上のガロワ拡大 F で以下に述べる特殊な型のものについて Leopoldt の予想が正しいことを示す。

次の記法を用いる：

(i) General quaternion group $\mathfrak{Q}_n$ of order 2^{n+1} $(n \geqq 2)$.

$$\mathfrak{Q}_n = \langle a_n, b \rangle : (a_n)^{2^n} = 1,\ b^2 = (a_n)^{2^{n-1}},\ b^{-1} a_n b = a_n^{-1};$$

(ii) Dihedral group $\mathfrak{D}_n$ of order 2^{n+1} $(n \geqq 2)$.

$$\mathcal{D}_n = \langle a_n, c \rangle : (a_n)^{2^n} = c^2 = 1,\ c^{-1} a_n c = a_n^{-1};$$

(iii) Quasi-dihedral group $\widetilde{\mathcal{D}}_n$ of order 2^{n+1} $(n \geqq 3)$.

$$\widetilde{\mathcal{D}}_n = \langle a_n, d \rangle : (a_n)^{2^n} = d^2 = 1,\quad d^{-1} a_n d = (a_n)^{-1+2^{n-1}}.$$

以下ではFを次のものとする:

(☆) Fは虚2次体k上のガロワ拡大F_1, F_2の合併体$F_1 \cdot F_2$であり,

(1) $F_1/\mathbb{Q}$はアーベル拡大で, アーベル群$\mathrm{Gal}(F_1/\mathbb{Q})$のexponentが奇数または$2\times$(奇数)であるもの;

(2) $F_2/\mathbb{Q}$はガロワ拡大で, $\mathfrak{G} = \mathrm{Gal}(F_2/\mathbb{Q})$とその正規部分群$\mathfrak{G}_1 = \mathrm{Gal}(F_2/k)$が次の(2-1)~(2-5)のいずれかの場合に属するものである。

(2-1) $\mathfrak{G} = \langle a, b, c \rangle : a^4 = c^2 = 1,\ b^2 = a^2,\ b^{-1} a b = a^{-1},$

$$c^{-1} a c = b.$$

$$\mathfrak{G}_1 = \langle a, b \rangle$$

(2-2) $\mathfrak{G} = \mathfrak{G}_{n+1} = \langle a_{n+1}, b \rangle$ $(n \geqq 2)$,

$$\mathfrak{G}_1 = \mathfrak{G}_n = \langle a_n, b \rangle;\ a_n = (a_{n+1})^2.$$

(2-3) $\mathfrak{G} = \mathcal{D}_{n+1} = \langle a_{n+1}, c \rangle$ $(n \geqq 2)$,

$$\mathfrak{G}_1 = \mathcal{D}_n = \langle a_n, c \rangle;\ a_n = (a_{n+1})^2.$$

(2-4) $\mathfrak{G} = \widetilde{\mathcal{D}}_{n+1} = \langle a_{n+1}, d \rangle$ $(n \geqq 2)$

$$\mathfrak{G}_1 = \mathfrak{G}_n = \langle a_n, b \rangle;\ a_n = (a_{n+1})^2,\ b = d\, a_{n+1}.$$

$$(2\text{-}5)\quad \mathfrak{g} = \tilde{\mathfrak{d}}_{n+1} = \langle a_{n+1}, d \rangle \quad (n \geqq 2).$$

$$\mathfrak{g}_1 = \mathfrak{d}_n = \langle a_n, c \rangle ; \quad a_n = (a_{n+1})^2, \ c = d.$$

すでに $G_1 = Gal(F/k)$ に関しては, $End_{\mathbb{Q}}(V)$, $(V = \mathfrak{O}_F^{\times} \otimes_{\mathbb{Z}} \mathbb{Q})$ における $\rho(\mathbb{Q}[G_1])$ の可換子環 $\widetilde{\rho(\mathbb{Q}[G_1])}$ の構造は定理3によって判明している。以下では上の場合について，今度は $G = Gal(F/\mathbb{Q})$ に関して，$\rho(\mathbb{Q}[G])$ の $End_{\mathbb{Q}}(V)$ における可換子環 $\widetilde{\rho(\mathbb{Q}[G])}$ が可換であり，$\rho(\mathbb{Q}[G])$ の中心と一致することを見る。しからば命題2，定理2，命題4が適用されるわけである。

自然数 ν に対して ζ_ν を 1 の原始 2^ν 乗根とし，

$$\tau_\nu = \zeta_\nu + \zeta_\nu^{-1}, \quad \lambda_\nu = \zeta_\nu - \zeta_\nu^{-1}$$

とおく。このとき $\nu \geqq 2$ ならば

$$[\mathbb{Q}(\zeta_\nu) : \mathbb{Q}(\tau_\nu)] = [\mathbb{Q}(\zeta_\nu) : \mathbb{Q}(\lambda_\nu)] = 2,$$

$$\mathbb{Q}(\zeta_\nu) = \mathbb{Q}(\tau_\nu, \sqrt{-1}),$$

$$[\mathbb{Q}(\lambda_\nu) : \mathbb{Q}(\tau_{\nu-1})] = 2$$

である。また $\mathbb{Q}(\tau_\nu)$ は総実，$\mathbb{Q}(\lambda_\nu)$ は総虚である。

次の4つの命題は容易にたしかめられるであろう。

<u>命題 8-1.</u> $\mathfrak{d}_n = \langle a_n, c \rangle \ (n \geqq 2)$ について

$$\mathbb{Q}[\mathfrak{d}_n] \cong \mathbb{Q}^4 \oplus \bigoplus_{\nu=2}^{n} M_2(\mathbb{Q}(\tau_\nu)).$$

ただし $\mathbb{Q}^4 = \overbrace{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}^{4\text{個}}$ は $\chi_i^{(n)} : \mathfrak{D}_n \to \mathbb{Q}^\times$ $(i = 0, 1, 2, 3)$

$$\chi_i^{(n)}(a_n) = (-1)^{\frac{i(i-1)}{2}}, \quad \chi_i^{(n)}(c) = (-1)^i$$

に対応し，$M_2(\mathbb{Q}(\tau_\nu))$ には $\xi_\nu^{(n)} : \mathfrak{D}_n \to GL_2(\mathbb{Q}(\tau_\nu))$

$$\xi_\nu^{(n)}(a_n) = \begin{pmatrix} 0 & -1 \\ 1 & \tau_\nu \end{pmatrix}, \quad \xi_\nu^{(n)}(c) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

に対応する。特に $\mathrm{Ker}\, \xi_\nu^{(n)} = \langle (a_n)^{2^{n-\nu}} \rangle$ である。

<u>命題 8-2.</u> $\widetilde{\mathfrak{D}}_n = \langle a_n, d \rangle$ $(n \geqq 3)$ については

$$\mathbb{Q}[\widetilde{\mathfrak{D}}_n] \cong \mathbb{Q}^4 \oplus \bigoplus_{\nu=2}^{n-1} M_2(\mathbb{Q}(\tau_\nu)) \oplus M_2(\mathbb{Q}(\lambda_n))$$

ただし $\mathbb{Q}^4 \oplus \bigoplus_{\nu=2}^{n-1} M_2(\mathbb{Q}(\tau_\nu))$ は $\widetilde{\mathfrak{D}}_n / \langle (a_n)^{2^{n-1}} \rangle \cong \mathfrak{D}_{n-1}$ に対応し，$M_2(\mathbb{Q}(\lambda_n))$ は $\widetilde{\xi}^{(n)} : \widetilde{\mathfrak{D}}_n \to GL_2(\mathbb{Q}(\lambda_n))$

$$\widetilde{\xi}^{(n)}(a_n) = \begin{pmatrix} 0 & 1 \\ 1 & \lambda_n \end{pmatrix}, \quad \widetilde{\xi}^{(n)}(d) = \begin{pmatrix} 1 & 0 \\ \lambda_n & -1 \end{pmatrix}$$

に対応している。

<u>命題 8-3.</u> $\mathfrak{Q}_n = \langle a_n, b \rangle$ $(n \geqq 2)$ については

$$H = \{\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k \mid \alpha, \beta, \gamma, \delta \in \mathbb{Q}\}$$

$$i^2 = j^2 = -1, \quad ij = -ji = k$$

とするとき

$$\mathbb{Q}[\mathfrak{Q}_n] \cong \mathbb{Q}^4 \oplus \bigoplus_{\nu=2}^{n-1} M_2(\mathbb{Q}(\tau_\nu)) \oplus H \otimes_{\mathbb{Q}} \mathbb{Q}(\tau_n).$$

ただし $\mathbb{Q}^4 \oplus \bigoplus_{\nu=2}^{n-1} M_2(\mathbb{Q}(\tau_\nu))$ $(n=2$ のときは $\mathbb{Q}^4)$ は

$\mathfrak{G}_n / \langle (a_n)^{2^{n-1}} \rangle \simeq \mathfrak{D}_{n-1}$ に対応し，$H \otimes_{\mathbb{Q}} \mathbb{Q}(\tau_n)$ は

$$\eta^{(n)} : \mathfrak{G}_n \longrightarrow (H \otimes_{\mathbb{Q}} \mathbb{Q}(\tau_n))^\times$$

$$\eta^{(n)}(a_n) = \frac{1}{2}(\tau_n - \tau_n' \cdot i), \quad \eta^{(n)}(b) = j$$

$$\tau_n' = \zeta_n^{1+2^{n-2}} + \zeta_n^{-1-2^{n-2}} \in \mathbb{Q}(\tau_n)$$

に対応する。

<u>命題 8－4</u>. (2-1) の群 $\mathfrak{G} = \langle a, b, c \rangle$ について

$$\mathbb{Q}[\mathfrak{G}] \cong \mathbb{Q}^4 \oplus M_2(\mathbb{Q}) \oplus M_4(\mathbb{Q}).$$

ただし $\mathbb{Q}^4$ は $(2,2)$ 型アーベル群 $\mathfrak{G}/\mathfrak{G}' = \mathfrak{G}/\langle a^{-1}b \rangle$ に対応し，$M_2(\mathbb{Q})$ は $\psi_1 : \mathfrak{G} \longrightarrow GL_2(\mathbb{Q})$

$$\psi_1(a) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \psi_1(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \psi_1(c) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

に対応し（$\mathrm{Ker}\,\psi_1 = \langle a^2 \rangle$），$M_4(\mathbb{Q})$ には $\psi_2 : \mathfrak{G} \to GL_4(\mathbb{Q})$

$$\psi_2(a) = \left(\begin{array}{cc|cc} & -1 & & \\ 1 & & & \\ \hline & & & 1 \\ & & -1 & \end{array}\right), \quad \psi_2(b) = \left(\begin{array}{cc|cc} & & -1 & \\ & & & -1 \\ \hline 1 & & & \\ & 1 & & \end{array}\right), \quad \psi_2(c) = \left(\begin{array}{c|cc|c} 0 & & & 1 \\ \hline & -1 & 0 & \\ & 0 & 1 & \\ \hline 1 & & & 0 \end{array}\right)$$

が対応する。

さて $F = F_1 \cdot F_2$ が条件(☆)を満たしているとき $Gal(F_1/\mathbb{Q})$ の exponent に関する仮定から，適当に F_1 の部分体 F_1' をとれば $F_1 = (F_1 \cap F_2) \cdot F_1'$ かつ $F_1' \cap F_2 = \mathbb{Q}$ となるようにできる。したがって F_1 と F_1' とをとりかえて，以後 $F_1 \cap F_2 =$

$\mathbb{Q}$とする。このとき $G=Gal(F/\mathbb{Q})\cong\mathfrak{A}\times\mathfrak{G}$, $G_1=Gal(F/k)\cong\mathfrak{A}\times\mathfrak{G}_1$, $\mathfrak{A}=Gal(F_1/\mathbb{Q})$, $\mathfrak{G}=Gal(F_2/\mathbb{Q})$, $\mathfrak{G}_1=Gal(F_2/k)$ である。しかもやはりアーベル群 $\mathfrak{A}$ の exponent はある $m=2\cdot m_0+1$ に対して m または $2\cdot m$ である。

次に $\mathbb{Q}[\mathfrak{G}_1]$ を、可換な準単純環 B_0 と、非可換な単純環 $B_1,\cdots,B_s$ との直和に分解し、B_j の単位元を e_j $(j=0,\cdots,s)$ とする。自然に $\mathbb{Q}[\mathfrak{G}_1]\subset\mathbb{Q}[\mathfrak{G}]$ と見るとき、$\mathfrak{G},\mathfrak{G}_1$ が (2-1)〜(2-5) に属するならば、非可換単純環 B_j $(1\leq j\leq s)$ に対しては $\mathbb{Q}[\mathfrak{G}]$ の唯一つの単純因子が唯一つの B_j を含んでおり、$\mathbb{Q}[\mathfrak{G}]$ の直和分解

$$\mathbb{Q}[\mathfrak{G}]=B_0'\oplus B_1'\oplus\cdots\oplus B_s',\quad (B_j'=e_j\cdot\mathbb{Q}[\mathfrak{G}])$$

において、$B_1',\cdots,B_s'$ は単純である。

一方 m の約数 μ に対して 1の原始 μ 乗根 ζ_μ' をとれば、$\mathbb{Q}[\mathfrak{A}]$ は $\mathbb{Q}(\zeta_\mu')$ $(\mu|m)$ なる体の直和である。(ただし一般に $\mathbb{Q}(\zeta_\mu')$ は各 $\mu|m$ について重複度をもってあらわれる。) したがって $\mathbb{Q}[G_1]\cong\mathbb{Q}[\mathfrak{A}]\otimes_{\mathbb{Q}}\mathbb{Q}[\mathfrak{G}_1]$, $\mathbb{Q}[G]\cong\mathbb{Q}[\mathfrak{A}]\otimes_{\mathbb{Q}}\mathbb{Q}[\mathfrak{G}]$ は、それぞれ、準単純環 $\mathbb{Q}[\mathfrak{A}]\otimes_{\mathbb{Q}}B_0$, $\mathbb{Q}[\mathfrak{A}]\otimes_{\mathbb{Q}}B_0'$, と単純環 $B_{j,\mu}=B_j\otimes_{\mathbb{Q}}\mathbb{Q}(\zeta_\mu')$, $B_{j,\mu}'=B_j'\otimes_{\mathbb{Q}}\mathbb{Q}(\zeta_\mu')$ $(j=1,\cdots,s;\mu|m)$ との直和に分解される。ここで $B_{j,\mu}$, $B_{j,\mu}'$ が単純であることは、それの中心は $\mathbb{Q}(\zeta_\nu)\otimes_{\mathbb{Q}}\mathbb{Q}(\zeta_\mu')$ に含まれるが、ζ_ν

は1の2^{ν}乗根でありζ'_μは奇数μに対する1のμ乗根であることから$\mathbb{Q}(\zeta_\nu)\otimes_{\mathbb{Q}}\mathbb{Q}(\zeta'_\mu)$が体になることがしたがい、保証されている。これらの直和因子は次の性質をもつ：

(イ) $\mathbb{Q}[\mathfrak{A}]\otimes_{\mathbb{Q}} B'_0$は可換な準単純環$\mathbb{Q}[\mathfrak{A}]\otimes_{\mathbb{Q}} B_0$を含む；

(ロ) (2-1)の場合は$s=1$で、$B_{1,\mu}$の中心と$B'_{1,\mu}$の中心とは一致し$\mathbb{Q}(\zeta'_\mu)$であり

$$[B_{1,\mu}:\mathbb{Q}(\zeta'_\mu)]=4,\quad [B'_{1,\mu}:\mathbb{Q}(\zeta'_\mu)]=4^2;$$

(ハ) (2-2)〜(2-5)の場合、$B_{j,\mu}$, $B'_{j,\mu}$の中心をそれぞれ$C_{j,\mu}$, $C'_{j,\mu}$とするとき

$$[C'_{j,\mu}:C_{j,\mu}]=2,\quad [B_{j,\mu}:C_{j,\mu}]=4,$$
$$B'_{j,\mu}=B_{j,\mu}\otimes_{C_{j,\mu}}C'_{j,\mu}.$$

さて$\mathrm{End}_{\mathbb{Q}}(V)$において$\rho(\mathbb{Q}[G_1])$, $\rho(\mathbb{Q}[G])$はそれぞれ$\rho(\mathbb{Q}[\mathfrak{A}]\otimes_{\mathbb{Q}} B_0)$, $\rho(B_{j,\mu})$および$\rho(\mathbb{Q}[\mathfrak{A}]\otimes B'_0)$, $\rho(B'_{j,\mu})$の直和に分解されるが、この$\rho(\mathbb{Q}[G_1])$の直和因子のひとつをB、その単位元をe、Bに対応する$\rho(\mathbb{Q}[G])$の直和因子をB'とするとき、eはB'の単位元でもある。さらにB, B'の$\mathrm{End}_{\mathbb{Q}}(e(V))$における可換子環を$\widehat{B}$, $\widehat{B'}$とすれば、$\widehat{B}$は$\widehat{B'}$を含んでいる。明らかに$\widehat{\rho(\mathbb{Q}[G_1])}$, $\widehat{\rho(\mathbb{Q}[G])}$はそれぞれ$\widehat{B}$, $\widehat{B'}$の直和に分解れる。我々の目標はどの$\widehat{B'}$も可換であることを示すことにある。まず$B=\rho(\mathbb{Q}[\mathfrak{A}]\otimes B_0)$の

とき，$\mathfrak{B}' = \rho(\mathbb{Q}[\mathfrak{A}] \otimes \mathfrak{B}_0')$ である。定理3により $\widetilde{\rho(\mathbb{Q}[G_1])}$ は $\rho(\mathbb{Q}[G_1])$ と同型であり，この同型により $\widetilde{\mathfrak{B}}$ は $\mathfrak{B}$ と同型になる。よって $\widetilde{\mathfrak{B}}$ は可換であり，それに含まれる $\widetilde{\mathfrak{B}'}$ も可換である。次に $\mathfrak{B} = \rho(B_{j,\mu})$，$\mathfrak{B}' = \rho(B'_{j,\mu})$ のときを見よう。この場合は $e(V)$ は $\mathfrak{B}'$ の中心 $C' = \rho(C'_{j,\mu})$ 上のベクトル空間と見なせ $\widetilde{\mathfrak{B}'}$ は $\mathrm{End}_{C'}(e(V))$ における $\mathfrak{B}'$ の可換子環となっている。定理3によれば $\mathbb{Q}$ 上のベクトル空間として $e(V)$ は $\mathfrak{B}$ と同型である。そこで $\mathfrak{B}$ の中心 $C = \rho(C_{j,\mu})$ 上のベクトル空間と見なして次元をしらべれば $\dim_C e(V) = 4$ である。したがって (2-1) の場合は (ロ) によって $\widetilde{\mathfrak{B}'} = C' = C$ となり，(2-2)～(2-5) の場合は (ハ) によって $\widetilde{\mathfrak{B}'} = C'$ となることは明らかである。ここに $\widetilde{\rho(\mathbb{Q}[G])}$ がその中心と一致して可換であることが示されたわけである。

よって命題2，定理2，および命題4にしたがい次の定理が得られる：

<u>定理5</u>　有理数体上のガロワ拡大体 F がある虚2次体 k を含み，(☆) を満たしているならば，F の部分体に対しては，すべての素数 p に対して Leopoldt の予想が正しい。

<u>注意</u>　群 $\mathfrak{G}_1$ を (i), (ii), (iii) のいずれかとするとき，群 $\mathfrak{G}$ で

$\mathfrak{G}_n / \langle (a_n)^{2^{n-1}} \rangle \cong \mathfrak{D}_{n-1}$ に対応し, $H \underset{\mathbb{Q}}{\otimes} \mathbb{Q}(\tau_n)$ は
$\eta^{(n)} : \mathfrak{G}_n \longrightarrow (H \underset{\mathbb{Q}}{\otimes} \mathbb{Q}(\tau_n))^{\times}$

$$\eta^{(n)}(a_n) = \frac{1}{2}(\tau_n - \tau_n' \cdot i), \quad \eta^{(n)}(b) = j$$

$$\tau_n' = \zeta_n^{1+2^{n-2}} + \zeta_n^{-1-2^{n-2}} \in \mathbb{Q}(\tau_n)$$

に対応する。

<u>命題 8−4</u>. (2-1) の群 $\mathfrak{G} = \langle a, b, c \rangle$ について

$$\mathbb{Q}[\mathfrak{G}] \cong \mathbb{Q}^4 \oplus M_2(\mathbb{Q}) \oplus M_4(\mathbb{Q}).$$

ただし $\mathbb{Q}^4$ は (2, 2) 型アーベル群 $\mathfrak{G}/\mathfrak{G}' = \mathfrak{G}/\langle a^{-1}b \rangle$ に対応し, $M_2(\mathbb{Q})$ は $\psi_1 : \mathfrak{G} \longrightarrow GL_2(\mathbb{Q})$

$$\psi_1(a) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \psi_1(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \psi_1(c) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

に対応し ($\mathrm{Ker}\, \psi_1 = \langle a^2 \rangle$), $M_4(\mathbb{Q})$ には $\psi_2 : \mathfrak{G} \to GL_4(\mathbb{Q})$

$$\psi_2(a) = \left(\begin{array}{cc|cc} & -1 & & \\ 1 & & & \\ \hline & & & 1 \\ & & -1 & \end{array}\right), \quad \psi_2(b) = \left(\begin{array}{cc|cc} & & -1 & \\ & & & -1 \\ \hline 1 & & & \\ & 1 & & \end{array}\right), \quad \psi_2(c) = \left(\begin{array}{c|cc|c} 0 & & & 1 \\ \hline & -1 & 0 & \\ & 0 & 1 & \\ \hline 1 & & & 0 \end{array}\right)$$

が対応する。

さて $F = F_1 \cdot F_2$ が条件 (☆) を満たしているとき $Gal(F_1/\mathbb{Q})$ の exponent に関する仮定から, 適当に F_1 の部分体 F_1' をとれば $F_1 = (F_1 \cap F_2) \cdot F_1'$ かつ $F_1' \cap F_2 = \mathbb{Q}$ となるようにできる。したがって F_1 と F_1' とをとりかえて, 以後 $F_1 \cap F_2 =$

$Gal(F_2/\mathbb{Q})$ なるとき ε_n が固定する F_2 の部分体 $\mathfrak{k}$ は実2次体であって，虚2次体ではあり得ない。

References

[1] J. Ax : On the units of an algebraic number field. Illinois J. Math., 9 (1965).

[2] A. Brumer : On the units of algebraic number field. Mathematica, 14 (1967).

[3] C. Chevalley : Deux théorèmes d'arithmétique. J. of Math. Soc. Japan, 3 (1951).

[4] J. Herbrand : Sur les unites d'un corps algébrique. Comptes rendue, 192 (1931), pp 24-27, p188.

[5] H. Leopoldt : Zur Arithmetik in abelschen Zahlkörpern, J. reine angew. Math., 209 (1962).